

ABSTRACT

A method includes establishing a SMTP proxy, defining an application that forms a connection with the SMTP proxy as a SMTP client application, emulating the SMTP client application including generating at least one SMTP client application dirty page, intercepting an executable application sent from the SMTP client application with the SMTP proxy, emulating the executable application including generating at least one executable application dirty page. If a determination is made that the at least one SMTP client application dirty page is a match and the at least one executable application dirty page, a determination is made that the SMTP client application is polymorphic malicious code that is attempting to send itself and protective action is taken.